SSL-ohje

(Secure Socket Layer)

Saat perustietoja verkosta ja Brother-laitteesi monipuolisista verkko-ominaisuuksista ohjeesta: ➤➤ Verkkokäyttäjän opas.

Voit ladata itsellesi uusimmat käyttöohjeet vierailemalla Brother Solutions Centerissä osoitteessa http://solutions.brother.com/. Sieltä voit ladata uusimmat ohjaimet ja apuohjelmat, lukea ohjeita vianetsintään, vastauksia usein esitettyihin kysymyksiin sekä lisätietoja tulostukseen liittyvistä erikoisominaisuuksista ja käyttömahdollisuuksista.

Mallien saatavuus vaihtelee maakohtaisesti.

Versio 0

FIN

Mallit

Tämä käyttöopas koskee seuraavia malleja.

HL-5450DN(T)/5470DW(T)/6180DW(T)

DCP-8110DN/8150DN/8155DN/8250DN/MFC-8510DN/8710DW/8910DW/8950DW(T)

Oppaassa käytetyt kuvakkeet

Tässä käyttöoppaassa käytetään seuraavia kuvakkeita:

Vinkki	Vinkki kertoo, miten toimia tietyissä tilanteissa, tai antaa vinkin siitä, miten valittu toiminto toimii yhdessä muiden toimintojen kanssa.

Tavaramerkit

Brother-logo on tavaramerkki, jonka omistaa Brother Industries, Ltd.

Microsoft, Windows, Windows Server ja Internet Explorer ovat Microsoft Corporationin rekisteröityjä tavaramerkkejä tai tavaramerkkejä Yhdysvalloissa ja/tai muissa maissa.

Windows Vista on Microsoft Corporationin tavaramerkki tai rekisteröity tavaramerkki Yhdysvalloissa ja/tai muissa maissa.

Jokaisella yrityksellä, jonka ohjelmiston nimi on mainittu tässä käyttöohjeessa, on omistamiaan sovelluksia koskeva käyttöoikeussopimus.

Kaikki Brotherin tuotteissa, niihin liittyvissä asiakirjoissa ja muissa materiaaleissa esiintyvät yritysten tavaramerkit ja tuotemerkit ovat kyseisten yritysten rekisteröityjä tavaramerkkejä.

TÄRKEÄ HUOMAUTUS

- Tämä tuote on hyväksytty käytettäväksi vain sen ostomaassa. Älä käytä tätä tuotetta sen ostomaan ulkopuolella, sillä se saattaa rikkoa kyseisen maan langatonta tietoliikennettä ja sähköturvallisuutta koskevia lakeja.
- Tässä oppaassa on käytetty MFC-8950DW(T) -mallin ruutuja, ellei muuta erikseen mainita.
- Tässä asiakirjassa Windows® XP tarkoittaa käyttöjärjestelmiä Windows® XP Professional, Windows® XP Professional x64 Edition ja Windows® XP Home Edition.
- Windows Server® 2003 tarkoittaa tässä asiakirjassa käyttöjärjestelmiä Windows Server® 2003 ja Windows Server® 2003 x64 Edition.
- Windows Server® 2008 tarkoittaa tässä asiakirjassa käyttöjärjestelmiä Windows Server® 2008 ja Windows Server® 2008 R2.
- Tässä oppaassa Windows Vistalla tarkoitetaan kaikkia Windows Vista® -versioita.
- Tässä oppaassa Windows® 7 tarkoittaa kaikkia Windows® 7 -versioita.
- Voit ladata muut ohjeet siirtymällä Brother Solutions Centeriin osoitteessa http://solutions.brother.com/ ja napsauttamalla oman mallisi sivulla Käyttöohjeet.

Sisällysluettelo

1 Johdanto

Yleistä

SSL (Secure Socket Layer) on tehokas tapa suojata paikallista tai laajaa verkkoliikennettä. Käytäntö salaa verkon kautta lähetettyä tietoa, kuten tulostustyön, joten tiedon kaappaamista yrittävät osapuolet eivät pysty lukemaan tietoa.

Salaus voidaan määrittää sekä langallisiin että langattomiin verkkoihin ja se toimii myös muiden suojausmenetelmien, kuten WPA-avainten ja palomuurien kanssa.

SSL:n lyhyt historiikki

SSL luotiin alunperin suojaamaan verkkoliikennettä, erityisesti selainten ja palvelinten välistä tiedonsiirtoa.

Jos käytät esimerkiksi Internet Explorer® WWW-selainta pankkiasiointiin verkossa, ja näet ”https://” -polun sekä pienen riippulukkokuvakkeen selaimesi osoitepalkissa, SSL on käytössä. Sittemmin SSL-käytäntöä ryhdyttiin käyttämään muissa sovelluksissa, kuten Telnetissä, tulostimissa ja FTP-sovelluksissa kehittyen siten verkkoturvallisuuden yleiskäytännöksi. Käytännön alkuperäiset periaatteet ovat edelleen käytössä useissa verkkokaupoissa ja pankeissa suojaamassa henkilökohtaisia tietoja, kuten luottokorttinumeroita, asiakashistorioita, jne.

SSL käyttää äärimmäisen korkeatasoista salausmenetelmää, johon luottaa useat pankit ympäri maailman, koska salausta lienee mahdotonta purkaa.

SSL:n edut

Suurin etu, kun käytetään SSL:ää Brother-laitteiden kanssa, on IP-verkon kautta tapahtuvan tulostuksen suojaus rajoittamalla luvattomien käyttäjien päästä käsiksi dataan, jota lähetetään laitteeseen. Laitteen myyntivaltti on se, että sitä voidaan käyttää salaisten tietojen tulostamiseen turvallisesti. Esimerkiksi suuren yrityksen henkilöstöosasto voi tulostaa palkkakuitteja säännöllisesti. Ilman suojausta verkon muut käyttäjät pystyvät lukemaan palkkakuittien sisältöä. SSL takaa sen, että tiedon luvaton kaappaus tuottaa ainoastaan epämääräisen sivun koodia, eikä todellista palkkakuittia.

Varmenteiden käyttäminen laitteen suojaamiseksi

Brother-laitteesi tukee useiden suojausvarmenteiden käyttämistä, joten laitteen hallinta, todennus ja tiedonsiirto on turvallisia. Laitteessa voidaan käyttää seuraavia suojausvarmenteiden ominaisuuksia. Kun tulostat asiakirjoja tai käytät WWW-pohjaista hallintaa (WWW-selain) suojatusti SSL:n avulla, sinun on asennettava varmenne tietokoneellesi. Katso *Digitaalisen varmenteen asennus* ➤➤ sivulla 4.

- SSL/TLS-tietoliikenne
- SSL-tietoliikenne SMTP/POP3-palvelimille

Brother-laite tukee seuraavia varmenteita.

- Esiasennettu varmenne

  Laitteessasi on esiasennettu ja itse allekirjoitettu varmenne.

  Tätä varmennetta käyttämällä voit käyttää SSL/TLS-yhteyttä helposti ilman varmenteen luomista tai asentamista. Jos haluat käyttää laitteesi Google Cloud Print -ominaisuutta, voit käyttää tätä esiasennettua varmennetta määrittääksesi Google Cloud Print -asetukset turvallisesti. Saadaksesi lisätietoja Google Cloud Print -ominaisuudesta, siirry Brother Solutions Centeriin osoitteessa http://solutions.brother.com/ ja napsauta Käyttöohjeet oman malliisi sivulla ladataksesi Google Cloud Print -opas.

Vinkki

Esiasennettu ja esiallekirjoitettu varmenne ei voi suojella verkkoliikennettä huijauksilta. Suosittelemme käyttämään varmennetta, jonka on julkaissut luotettava tekijä paremman turvallisuuden vuoksi.

- Itse allekirjoitettu varmenne

  Tämä tulostuspalvelin myöntää oman varmenteensa. Tätä varmennetta käyttämällä voit käyttää SSL/TLS-yhteyttä helposti ilman CA:n myöntämää varmennetta. (Katso *Itse allekirjoitetun varmenteen luominen* ➤➤ sivulla 6.)

- CA:n myöntämä varmenne

  CA:n myöntämän varmenteen voi asentaa kahdella tavalla. Jos sinulla on jo CA-varmenne tai jos haluat käyttää ulkopuolista luotettavaa CA:ta:

  - Käytettäessä CSR:ää (Certificate Signing Request) tästä tulostuspalvelimesta. (Katso *Sertifikaatin allekirjoituspyynnön (CSR) luominen* ➤➤ sivulla 7.)
  - Tuotaessa varmenne ja yksityinen avain. (Katso *Varmenteen ja yksityisen avaimen tuominen ja vieminen* ➤➤ sivulla 17.)

■ CA-varmenne

Jos käytät CA:n (Certificate Authority) itse yksilöivää CA-varmennetta, sinun on tuotava CA-varmenne CA:lta ennen määritysten tekemistä. (Katso *CA-varmenteen tuominen ja vieminen* ➤➤ sivulla 18.)

Vinkki

- Jos aiot käyttää SSL/TLS-yhteyttä, on suositeltavaa ottaa yhteyttä järjestelmänvalvojaan ennen käyttöä.
- Jos palautat tulostuspalvelimen tehdasasetukset, palvelimeen asennetut varmenne ja yksityinen avain poistetaan. Jos haluat säilyttää varmenteen ja yksityisen avaimen tulostuspalvelimen palautuksen yhteydessä, vie ne palvelimesta ennen palautusta ja asenna ne sitten uudelleen. (Katso *Itse allekirjoitetun varmenteen, CA:n myöntämän varmenteen ja yksityisen avaimen tuominen* ➤➤ sivulla 17.)

2 SSL-verkkoliikenteen digitaalinen varmenne

Digitaalisen varmenteen asennus

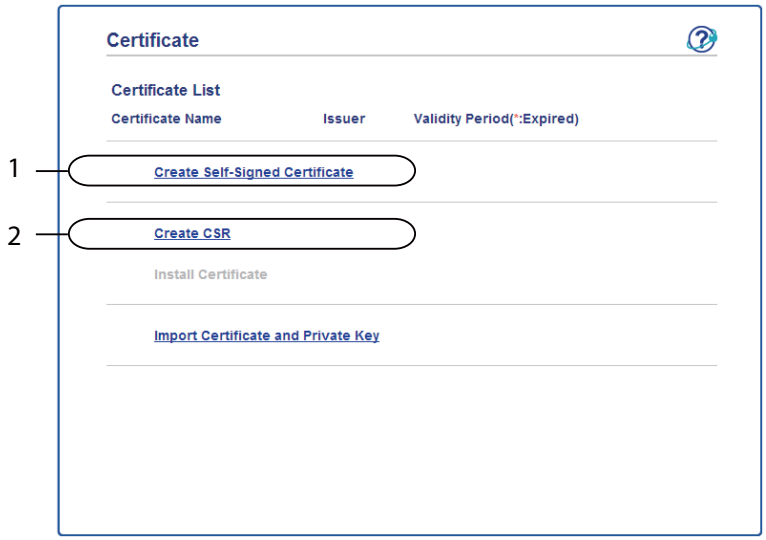
Tulostaminen suojatun verkon yli tai suojattu hallinta Web-pohjaista hallintaa (WWW-selain) käyttäen, vaatii digitaalisen varmenteen asentamisen sekä laitteeseen että tietoa lähettävään laitteeseen, kuten esimerkiksi tietokoneeseen. Laitteessasi on esiasennettu varmenne. Varmenteen määrittämiseksi käyttäjän on kirjauduttava sisään laitteeseen WWW-selaimen kautta käyttämällä laitteen IP-osoitetta.

Vinkki

Suosituksena on Windows® Internet Explorer® 7.0/8.0 tai Firefox® 3.6 (Windows®) ja Safari 4.0/5.0 (Macintosh). Varmista myös, että JavaScript ja evästeet ovat käytössä käyttämässäsi selaimessa. Jos käytössä on jokin muu selain, sen on oltava yhteensopiva HTTP 1.0:n ja HTTP 1.1:n kanssa.

1. Käynnistä WWW-selain.
2. Kirjoita selaimen osoitepalkkiin ”http://laitteen IP-osoite/” (jossa ”laitteen IP-osoite” on laitteen IP-osoite tai tulostuspalvelimen nimi).
   - Esimerkiksi: http://192.168.1.2/
3. Salasanaa ei oletusarvon mukaan tarvita. Jos olet määrittänyt salasanan aiemmin, syötä se ja paina .
4. Valitse **Network** (Verkko).
5. Valitse **Security** (Suojaus).
6. Valitse **Certificate** (Sertifikaatti).

7 Voit määrittää sertifikaatin asetukset.
Luodaksesi itse allekirjoitettu varmenne Web-pohjaisella hallinnalla, siirry kohtaan *Itse allekirjoitetun varmenteen luominen* ➤➤ sivulla 6.
Luodaksesi sertifikaatin allekirjoituspyynnön (Certificate Signing Request, CSR), siirry kohtaan *Sertifikaatin allekirjoituspyynnön (CSR) luominen* ➤➤ sivulla 7.



1 Itse allekirjoitetun varmenteen luominen ja asentaminen

2 Certificate Authority (CA) -varmenteen käyttö

Vinkki

- Harmaana näkyvät, linkittämättömät toiminnot eivät ole käytettävissä.
- Katso lisätietoja asetusten määrittämisestä Web-pohjaisen hallinnan Ohjeesta.

Itse allekirjoitetun varmenteen luominen

1. Valitse **Create Self-Signed Certificate** (Luo itse allekirjoitettu varmenne).
2. Syötä **Common Name** (Yleinen nimi) ja **Valid Date** (Kelpoisuuspäivä).

Vinkki

- **Common Name** (Yleinen nimi) -pituuden on oltava alle 64 merkkiä. Kirjoita tunniste, kuten IP-osoite tai solmun tai toimialueen nimi, kun muodostat laitteeseen SSL/TLS-yhteyden. Solmun nimi on oletusarvoisesti näkyvissä.
- Näkyviin tulee varoitus, jos käytät IPPS- tai HTTPS-protokollaa ja kirjoitat osoitekenttään eri nimen kuin kohtaan **Common Name** (Yleinen nimi), jota käytettiin itse allekirjoitetussa varmenteessa.

3. Voit valita alasvetovalikosta **Public Key Algorithm** (Julkisen avaimen algoritmi)- ja**Digest Algorithm** (Digest-algoritmi) -asetukset. **Public Key Algorithm** (Julkisen avaimen algoritmi) -oletusasetus on **RSA(2048bit)** (RSA (2048-bittinen)) ja **Digest Algorithm** (Digest-algoritmi) -oletusasetus on **SHA256**.
4. Valitse **Submit** (Lähetä).
5. Itse allekirjoitettu varmenne on nyt luotu ja tallennettu laitteen muistiin.

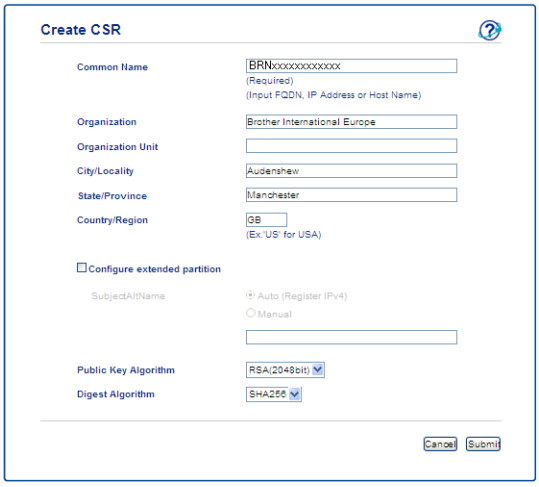
Sertifikaatin allekirjoituspyynnön (CSR) luominen

Sertifikaatin allekirjoituspyyntö (CSR) lähetetään CA:lle sertifikaatin sisältävien valtuustietojen varmentamiseksi.

Vinkki

On suositeltavaa asentaa CA:n päävarmenne tietokoneeseen ennen CSR:n luomista.

1. Valitse **Create CSR** (Luo CSR).
2. Kirjoita **Common Name** (Yleinen nimi) ja omat tietosi, kuten **Organization** (Organisaatio). Sinun on toimitettava yrityksesi tiedot, jotta CA voi varmistaa henkilöllisyytesi ja vahvistaa tämän maailmanlaajuisesti.



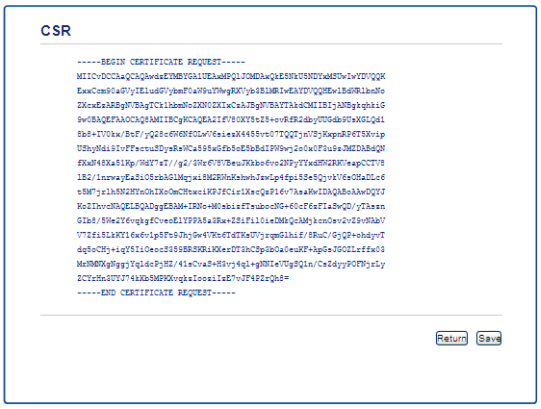
Vinkki

- **Common Name** (Yleinen nimi) -pituuden on oltava alle 64 merkkiä. Kirjoita tunniste, kuten IP-osoite tai solmun tai toimialueen nimi, kun muodostat laitteeseen SSL/TLS-yhteyden. Solmun nimi on oletusarvoisesti näkyvissä. **Common Name** (Yleinen nimi) täytyy määrittää.
- Näkyviin tulee varoitus, jos kirjoitat URL-kenttään eri nimen kuin se yleinen nimi, jota käytettiin varmenteessa.
- Kohteiden **Organization** (Organisaatio), **Organization Unit** (Organisaation yksikkö), **City/Locality** (Paikkakunta) ja **State/Province** (Osavaltio tai provinssi) pituuksien on oltava alle 64 merkkiä.
- Kohdassa **Country/Region** (Maa tai alue) tulee olla kaksimerkkinen ISO 3166 -maatunnus.
- Jos määrität X.509v3-varmenteen jatketta, valitse **Configure extended partition** (Määritä laajennettu osio) -valintaruutu ja valitse sitten **Auto (Register IPv4)** (Automaattinen (rekisteröi IPv4)) tai **Manual** (Manuaalinen).

3 Voit valita alasvetovalikosta **Public Key Algorithm** (Julkisen avaimen algoritmi)- ja**Digest Algorithm** (Digest-algoritmi) -asetukset. **Public Key Algorithm** (Julkisen avaimen algoritmi) -oletusasetus on **RSA(2048bit)** (RSA (2048-bittinen)) ja **Digest Algorithm** (Digest-algoritmi) -oletusasetus on **SHA256**.

4 Valitse **Submit** (Lähetä). Seuraava näyttö aukeaa.

5 Hetken kuluttua saat sertifikaatin, joka voidaan tallentaa pieneen tiedostoon tai kopioida ja liittää suoraan CA:n tarjoamaan CSR-verkkolomakkeeseen. Napsauta **Save** (Tallenna) tallentaaksesi CSR-tiedoston tietokoneellesi.



Vinkki

Noudata CA-käytäntöä, kun lähetät CSR:n CA:llesi.

6 CSR on luotu. Ohjeita varmenteen asentamisesta laitteeseen on kohdassa *Varmenteen asentaminen laitteeseen* ➤➤ sivulla 9.

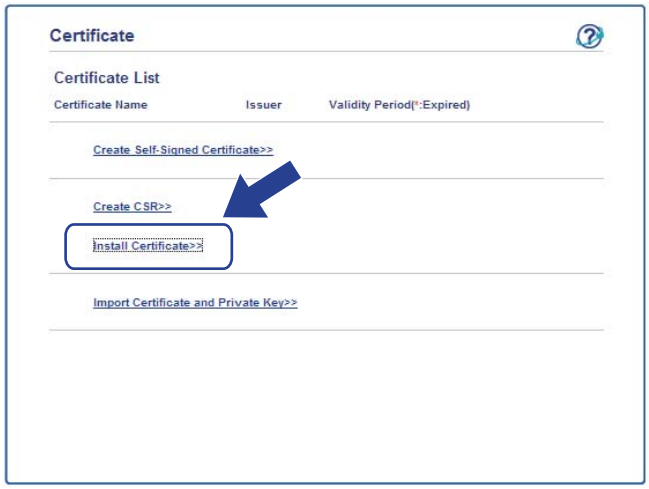
Varmenteen asentaminen laitteeseen

Kun saat varmenteen CA:lta, asenna se tulostuspalvelimeen seuraavien ohjeiden mukaan.

Vinkki

Vain tämän laitteen CSR:llä hankittu varmenne voidaan asentaa. Varmista ennen toisen CSR:n luomista, että varmenne on asennettu. Luo toinen CSR, kun olet asentanut varmenteen laitteeseen. Muussa tapauksessa ennen asennusta luotu CSR ei kelpaa.

1. Valitse **Install Certificate** (Asenna varmenne) sivulta **Certificate** (Sertifikaatti).



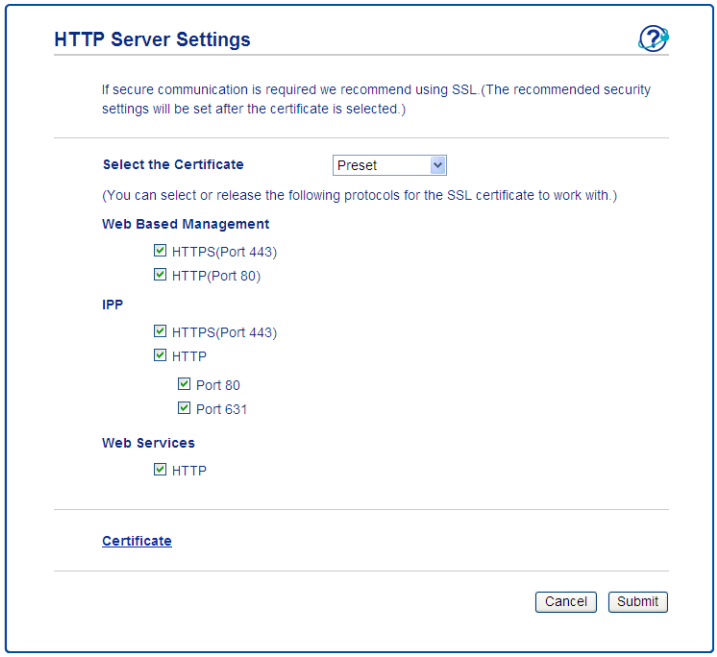
2. Valitse CA:n myöntämä varmennetiedosto ja valitse sitten **Submit** (Lähetä).

3. Varmenne on nyt luotu onnistuneesti ja tallennettu laitteen muistiin onnistuneesti.
SSL/TLS-yhteyden käyttäminen edellyttää, että CA:lta saatu päävarmenne on tallennettu tietokoneeseesi. Kysy asennusohjeita verkonvalvojalta.
Olet suorittanut digitaalisen varmenteen määrityksen. Jos haluat lähettää tai vastaanottaa sähköpostia SSL-tekniikan avulla, katso vaadittavat määritysvaiheet kohdasta *Sähköpostin lähettäminen tai vastaanottaminen suojatusti (DCP- ja MFC-mallit)* ➤➤ sivulla 25.

Varmenteen valinta

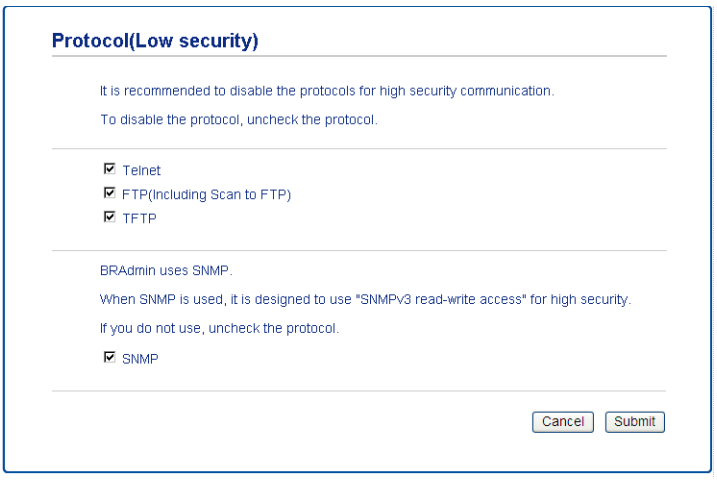
Kun olet asentanut varmenteen, noudata seuraavia vaiheita valitaksesi haluamasi varmenteen.

1. Valitse **Network** (Verkko).
2. Valitse **Protocol** (Protokolla).
3. Napsauta **HTTP Server Settings** (HTTP-palvelimen asetukset) ja valitse varmenne **Select the Certificate** (Valitse sertifikaatti) alasvetovalikosta.



Vinkki

- Jos seuraava valintaikkuna ilmestyy, Brother suosittelee poistamaan käytöstä Telnetin, FTP- ja TFTPprotokollat sekä BRAdmin Professionalin vanhempia versioita (versio 2,8 tai aiemmat) käyttävän verkkohallinnan turvallisen verkkoliikenteen varmistamiseksi. Jos otat edellä mainitut toiminnot käyttöön, käyttäjän todennus ei ole suojattu.



- DCP- ja MFC-mallit:

  Jos poistat FTP:n käytöstä, Skannaa FTP:lle toiminto poistetaan käytöstä.

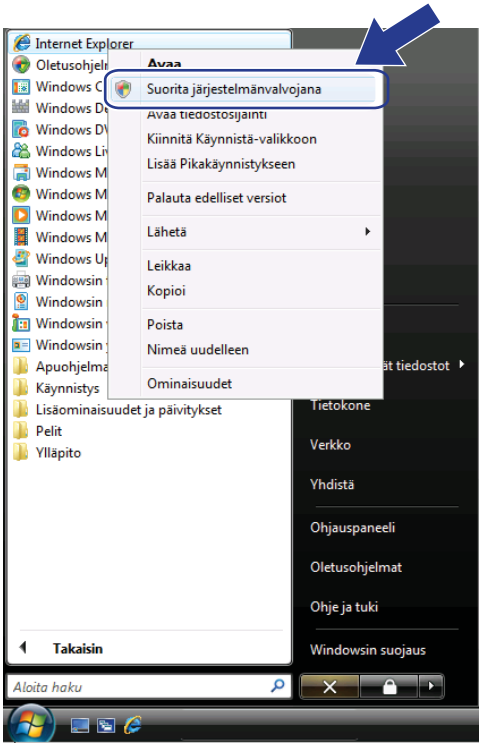
4 Valitse **Submit** (Lähetä).

Itse allekirjoitetun tai esiasennetun varmenteen asentaminen Windows Vista®, Windows® 7 ja Windows Server® 2008 -käyttöjärjestelmiin järjestelmänvalvojan oikeudet omaavien käyttäjien toimesta

Vinkki

- Seuraavat vaiheet koskevat Windows® Internet Explorer®-selainta. Jos käytät jotakin muuta selainta, nouda selaimen omia ohjeita.
- Sinulla on oltava järjestelmänvalvojan oikeudet asentaaksesi itse allekirjoitetun tai esiasennetun varmenteen.

1. Valitse ja **Kaikki ohjelmat**.
2. Napsauta hiiren kakkospainikkeella **Internet Explorer**-vaihtoehtoa ja valitse **Suorita järjestelmänvalvojana**.



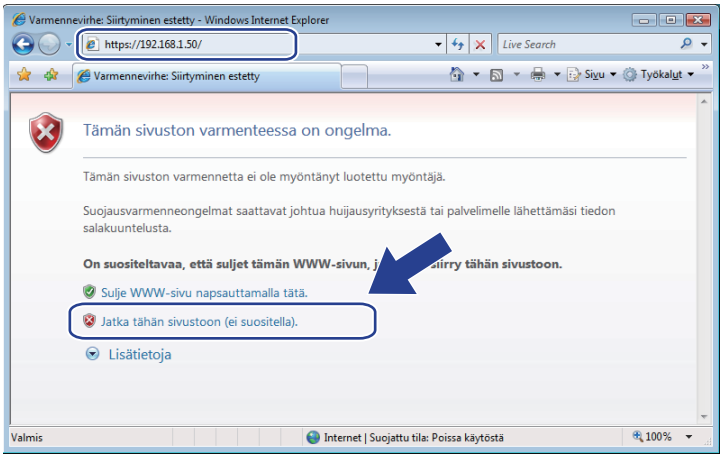
Vinkki

Jos **Käyttäjätilien valvonta** -näyttö tulee näkyviin,

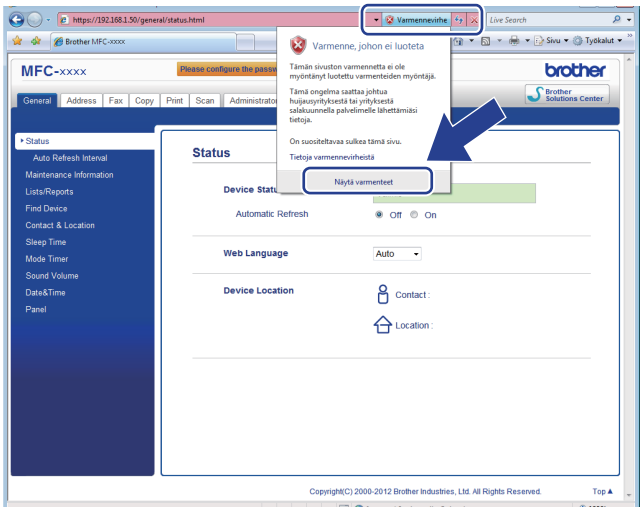
(Windows Vista®) Valitse **Jatka (Salli)**.

(Windows® 7) Valitse **Kyllä**.

3 Siirry laitteeseen kirjoittamalla selaimeen ”https://laitteen IP-osoite/” (jossa ”laitteen IP-osoite” on laitteen IP-osoite tai solmun nimi, joka määritettiin varmenteelle).
Valitse sitten **Jatka tähän sivustoon (ei suositella).**.

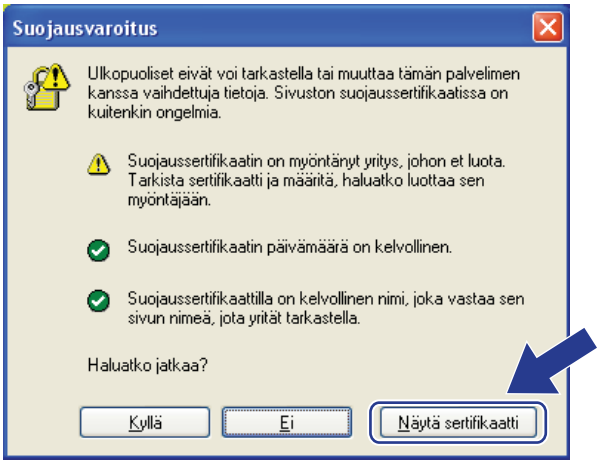


4 Valitse **Varmennevirhe** ja **Näytä varmenteet**. Seuraa jatko-ohjeita kohdan *Allekirjoitetun tai esiasennetun varmenteen asentaminen Windows® XP ja Windows Server® 2003 -käyttöjärjestelmiin* ➤➤ sivulla 14 vaiheesta 4.

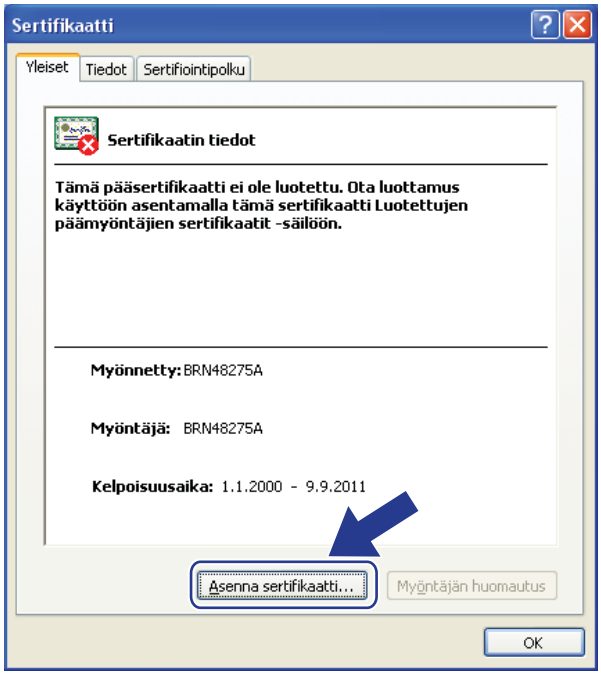


Allekirjoitetun tai esiasennetun varmenteen asentaminen Windows® XP ja Windows Server® 2003 -käyttöjärjestelmiin

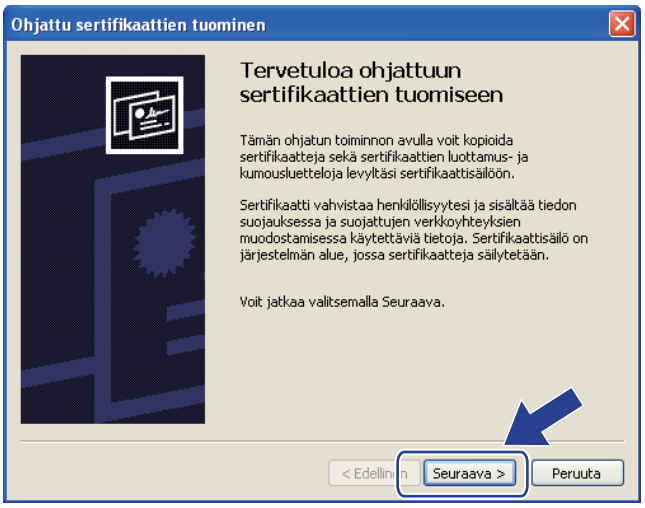
1. Käynnistä WWW-selain.
2. Siirry laitteeseen kirjoittamalla selaimeen ”https://laitteen IP-osoite/” (jossa ”laitteen IP-osoite” on IP-osoite tai solmun nimi, joka määritettiin varmenteelle).
3. Kun suojausvaroitusikkuna ilmestyy, toimi seuraavalla tavalla:
   - Valitse **Jatka tähän sivustoon (ei suositella).**. Valitse **Varmennevirhe** ja **Näytä varmenteet**.
   - Kun seuraava valintaikkuna tulee näkyviin, napsauta **Näytä sertifikaatti**.



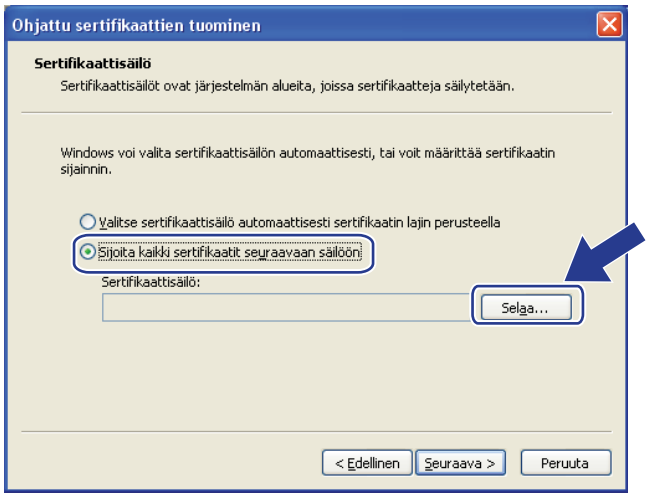
4. Valitse **Asenna sertifikaatti... Yleiset**-välilehdestä.



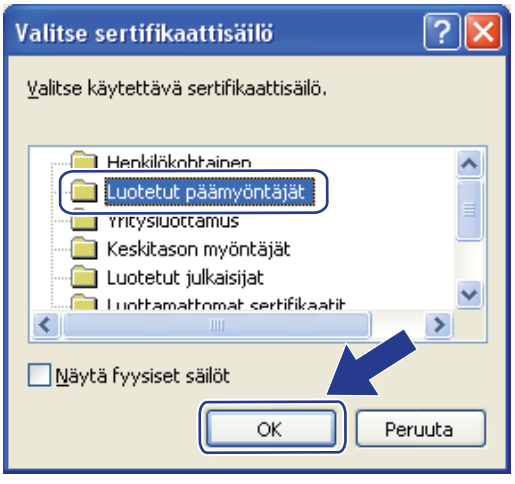
5 Kun **Ohjattu sertifikaattien tuominen** -ikkuna tulee näkyviin, napsauta **Seuraava**.



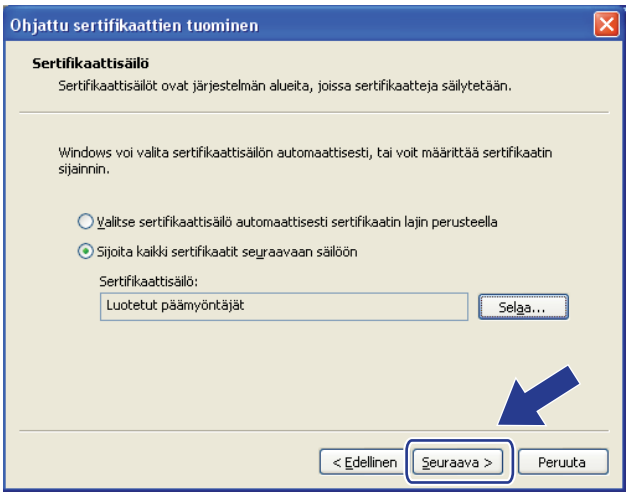
6 Sinun on määritettävä asennuspaikka varmenteelle. Suosittelemme, että valitset **Sijoita kaikki sertifikaatit seuraavaan säilöön** ja napsauta sitten **Selaa...**.



7 Valitse **Luotetut päämyöntäjät** ja **OK**.



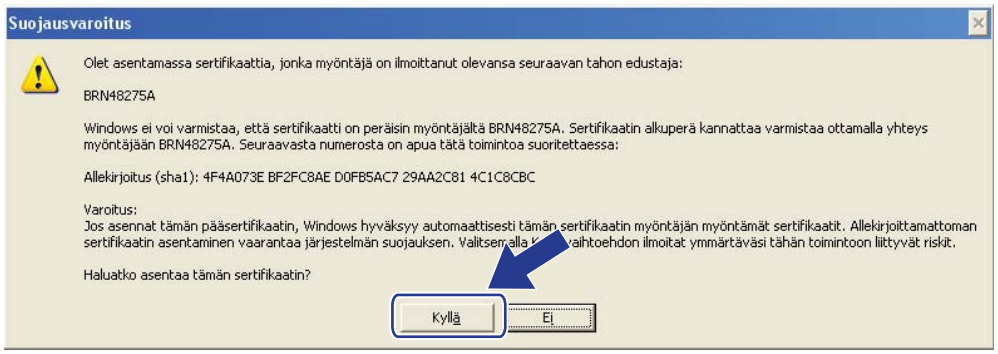
8 Napsauta **Seuraava**.



9 Napsauta seuraavassa näytössä **Valmis**.

10 Tämän jälkeen sinua pyydetään asentamaan varmenne.
Tee jokin seuraavista:

- Jos asennat itse allekirjoitettua varmennetta, vahvista tunnistetieto (allekirjoitus) ja napsauta **Kyllä**.
- Jos asennat esiasennettua varmennetta, napsauta **Kyllä**.



Vinkki

- Itse allekirjoitetussa varmenteessa tunnistetieto (allekirjoitus) näkyy verkkoasetusraportissa.

  Jos haluat lisätietoja verkkoasetusraportin tulostamisesta, katso *Tulostusasetukset-sivun tulostaminen (HL-5450DN(T))* ➤➤ sivulla 29 tai *Verkkoasetusraportin tulostaminen (muut mallit)* ➤➤ sivulla 29.
- Esiasennetussa varmenteessa tunnistetieto ei näy verkkoasetusraportissa.

11 Valitse **OK**.

12 Itse allekirjoitettu tai esiasennettu varmenne on asennettu tietokoneeseen ja SSL/TLS-yhteyttä voi käyttää.

Jokaisen suojatusti tulostavan tietokoneen on toimittava samoin. Näitä toimenpiteitä ei kuitenkaan tarvitse toistaa asennuksen jälkeen, ellei varmenne muutu.

Varmenteen ja yksityisen avaimen tuominen ja vieminen

Voit tallentaa varmenteen ja yksityisen avaimen laitteeseen ja hallita niitä tuomalla ja viemällä.

Itse allekirjoitetun varmenteen, CA:n myöntämän varmenteen ja yksityisen avaimen tuominen

1. Valitse **Import Certificate and Private Key** (Tuo varmenne ja yksityinen avain) sivulta **Certificate** (Sertifikaatti).
2. Valitse tuotava tiedosto.
3. Kirjoita salasana, jos tiedosto on salattu, ja valitse sitten **Submit** (Lähetä).
4. Varmenne ja yksityinen avain on nyt tuotu laitteeseesi.

Itse allekirjoitetun varmenteen, CA:n myöntämän varmenteen ja yksityisen avaimen vieminen

1. Valitse **Certificate** (Sertifikaatti) -sivulla **Certificate List** (Varmenneluettelo) -vaihtoehdon kanssa näkyvä **Export** (Vie).
2. Kirjoita salasana, jos haluat salata tiedoston.

Vinkki

Jos salasanaa ei kirjoiteta, tiedostoa ei salata.

3. Vahvista salasana kirjoittamalla se uudelleen ja valitse sitten **Submit** (Lähetä).
4. Valitse tiedostolle tallennuskohde.
5. Varmenne ja yksityinen avain on nyt viety tietokoneeseesi.

CA-varmenteen tuominen ja vieminen

Voit tuoda ja viedä CA-varmenteita ja tallentaa niitä laitteeseen.

CA-varmenteen tuominen

1. Valitse **CA Certificate** (CA-sertifikaatti) sivulta **Security** (Suojaus).
2. Valitse **Import CA Certificate** (Tuo CA-varmenne) ja valitse varmenne. Valitse **Submit** (Lähetä).

CA-varmenteen vieminen

1. Valitse **CA Certificate** (CA-sertifikaatti) sivulta **Security** (Suojaus).
2. Valitse varmenne, jonka haluat viedä, ja valitse **Export** (Vie). Valitse **Submit** (Lähetä).
3. Napsauta **Save** (Tallenna) valitaksesi kohdekansion.
4. Valitse kohde, johon haluat tallentaa viedyn varmenteen ja tallenna varmenne.

Useiden varmenteiden hallinta

Tämän useiden varmenteiden toiminnon avulla voit hallita kutakin varmennetta, jonka olet asentanut Web-pohjaisen hallinnan avulla. Kun olet asentanut varmenteet, voit tarkastella asennettuja varmenteita **Certificate** (Sertifikaatti) -sivulla ja tarkastella sitten kunkin varmenteen sisältöä sekä poistaa varmenteen tai viedä sen. Lisätietoja **Certificate** (Sertifikaatti) -sivun käytöstä: *Digitaalisen varmenteen asennus* ➤➤ sivulla 4.

- Tulostinmallit

  Brother-laitteen avulla voit tallentaa enintään kolme-neljä itse allekirjoitettua varmennetta tai enintään kolme-neljä CA:n myöntämää varmennetta. Voit käyttää tallennettuja varmenteita HTTP/IPPS-protokollaan tai IEEE 802.1x -todennukseen.

- DCP- ja MFC-mallit

  Brother-laitteen avulla voit tallentaa enintään neljä itse allekirjoitettua varmennetta tai enintään neljä CA:n myöntämää varmennetta. Voit käyttää tallennettuja varmenteita HTTP/IPPS-protokollaan, IEEE 802.1x -todennukseen tai allekirjoitettuun PDF-tiedostoon.

Voit myös tallentaa enintään neljä CA-varmennetta IEEE 802.1x -todennuksen sekä SMTP/POP3-palvelinten SSL-yhteyden käyttämistä varten.

Suosittelemme, että jätät yhden sertifikaatin tallentamatta ja säästät sen siltä varalta, että jokin varmenne umpeutuu. Jos esimerkiksi haluat tallentaa CA-varmenteen, tallenna kolme varmennetta ja yksi jää varalle. Jos varmenne myönnetään uudelleen esimerkiksi voimassaoloajan päättyessä, voit luoda uuden varmenteen varapaikkaan ja voit sitten poistaa umpeutuneen varmenteen määritysvian välttämiseksi.

Vinkki

- Jos käytät HTTPS/IPPS-, IEEE 802.1x- protokollaa tai allekirjoitettu PDF:ää (DCP- ja MFC-mallit), sinun on valittava, mitä varmennetta käytetään.
- Kun käytät SSL-tekniikkaa SMTP/POP3-tietoliikenteeseen (DCP- ja MFC-mallit), varmennetta ei tarvitse valita. Tarvittava varmenne valitaan automaattisesti.

3 Verkkolaitteen hallinta suojatusti SSL/TLS-yhteyden avulla

Verkkolaitteen turvallinen hallinta edellyttää, että hallinta-apuohjelmia käytetään suojausprotokollien kanssa.

Turvallinen hallinta WWW-pohjaisen hallinnan (Web-selaimen) avulla

On suositeltavaa käyttää HTTPS-protokollaa turvallisen hallinnan varmistamiseksi. Näiden protokollien käyttäminen edellyttää seuraavia laiteasetuksia.

Vinkki

- HTTPS-protokolla on oletusarvon mukaan käytössä.

  Voit muuttaa HTTPS-protokollan asetuksia sekä käytettävää varmennetta WWW-pohjaisen hallinnan näytössä valitsemalla ensin **Network** (Verkko), **Protocol** (Protokolla) ja sitten **HTTP Server Settings** (HTTP-palvelimen asetukset).
- Sinun on asennettava laitteeseen asennettu varmenne myös tietokoneeseesi. Katso *Itse allekirjoitetun tai esiasennetun varmenteen asentaminen Windows Vista®, Windows® 7 ja Windows Server® 2008 -käyttöjärjestelmiin järjestelmänvalvojan oikeudet omaavien käyttäjien toimesta* ➤➤ sivulla 12 tai *Allekirjoitetun tai esiasennetun varmenteen asentaminen Windows® XP ja Windows Server® 2003 -käyttöjärjestelmiin* ➤➤ sivulla 14.

1. Käynnistä WWW-selain.
2. Kirjoita ”https://laitteen IP-osoite/” selaimeen. (Jos käytät luotua varmennetta, kirjoita ”https://Yleinen nimi/” selaimeen. ”Yleinen nimi” on varmenteelle annettu yleinen nimi, kuten IP-osoite tai solmun tai toimialueen nimi. Jos haluat lisätietoja yleisen nimen antamisesta varmenteelle, katso *Varmenteiden käyttäminen laitteen suojaamiseksi* ➤➤ sivulla 2.)

   ■ Esimerkki:

   https://192.168.1.2/ (jos yleinen nimi on laitteen IP-osoite)
3. Salasanaa ei oletusarvon mukaan tarvita. Jos olet määrittänyt salasanan, anna se ja paina .

4 Asiakirjojen tulostaminen suojatusti SSL-yhteyden avulla

Asiakirjojen tulostaminen suojatusti Windowsin® IPPS-protokollan avulla

On suositeltavaa käyttää IPPS-protokollaa turvallisen hallinnan varmistamiseksi. IPPS-protokollan käyttäminen edellyttää seuraavia laiteasetuksia.

Vinkki

- IPPS-prokollan käyttäminen tietoliikenteessä ei estä tulostuspalvelimen luvatonta käyttöä.
- Sinun on asennettava laitteeseen asennettu varmenne myös tietokoneeseesi. Katso *Itse allekirjoitetun tai esiasennetun varmenteen asentaminen Windows Vista®, Windows® 7 ja Windows Server® 2008 -käyttöjärjestelmiin järjestelmänvalvojan oikeudet omaavien käyttäjien toimesta* ➤➤ sivulla 12 tai *Allekirjoitetun tai esiasennetun varmenteen asentaminen Windows® XP ja Windows Server® 2003 -käyttöjärjestelmiin* ➤➤ sivulla 14.
- IPPS-protokollan tulee olla käytössä. Oletusasetus on, että protokolla on käytössä. Voit muuttaa IPPS-protokollan asetuksia sekä käytettävää varmennetta WWW-pohjaisen hallinnan näytössä valitsemalla ensin **Network** (Verkko), **Protocol** (Protokolla) ja sitten **HTTP Server Settings** (HTTP-palvelimen asetukset).

Windows® XP ja Windows Server® 2003

1. Valitse **Käynnistä** ja valitse sitten **Tulostimet ja faksit**.
2. Napsauta **Lisää tulostin** aloittaaksesi **Ohjattu tulostimen asennus** -toiminnon.
3. Napsauta **Seuraava**, kun näet **Tervetuloa ohjattuun tulostimen asennukseen**-näytön.
4. Valitse **Verkkotulostin tai toiseen tietokoneeseen kytketty tulostin**.
5. Napsauta **Seuraava**.
6. Valitse **Yhdistä Internetissä tai paikallisessa verkossa olevaan tulostimeen** ja syötä seuraava osoite URL-kenttään:
”http://laitteen IP-osoite/ipp” (jossa ”laitteen IP-osoite” on laitteen IP-osoite tai solmun nimi).

Vinkki

- On tärkeää, että käytät muotoa ”https://” muodon ”http://” sijasta. Muutoin IPP:n kautta tulostaminen ei ole suojattua.
- Jos olet muokannut hosts-tiedostoa tietokoneellasi tai käytät Domain Name System (DNS) -järjestelmää, voit myös syöttää tulostuspalvelimen DNS-nimen. Koska tulostuspalvelin tukee TCP/IP:tä sekä NetBIOS-nimiä, voit myös syöttää tulostuspalvelimen NetBIOS-nimen. NetBIOS-nimi näkyy verkkoasetusraportissa. (Jos haluat lisätietoja verkkoasetusraportin tulostamisesta, katso *Tulostusasetukset-sivun tulostaminen (HL-5450DN(T))* ➤➤ sivulla 29 tai *Verkkoasetusraportin tulostaminen (muut mallit)* ➤➤ sivulla 29.) Annettu NetBIOS-nimi on silmukan nimen 15 ensimmäistä merkkiä, ja se näkyy oletusarvoisesti muodossa ”BRNxxxxxxxxxxxx” langallisessa verkossa tai ”BRWxxxxxxxxxxxx” langattomassa verkossa. (”xxxxxxxxxxxx” on laitteesi MAC-osoite/Ethernet-osoite.)

7. Kun napsautat **Seuraava**, Windows® XP ja Windows Server® 2003 muodostavat yhteyden määrittämääsi osoitteeseen.

   ■ Jos tulostinohjain on jo asennettu:

   Näet tulostimen valintanäytön kohdassa **Ohjattu tulostimen asennus**.

   Siirry vaiheeseen ⓫.

   ■ Jos tulostinohjainta EI OLE asennettu:

   Yksi IPP-tulostusprotokollan eduista on, että se määrittää tulostimen mallin nimen kun kommunikoit sen kanssa. Kun tiedonsiirto on onnistunut, näet tulostimen mallin nimen automaattisesti. Tämä merkitsee sitä, ettei sinun tarvitse ilmoittaa Windows® XP ja Windows Server® 2003 -järjestelmille käytettävää tulostimen ohjaintyyppiä.

   Siirry vaiheeseen ❽.

Vinkki

Jos asentamasi tulostin ei sisällä digitaalista varmennetta, näet varoitusviestin. Napsauta **Jatka asentamista** jatkaaksesi asennusta.

8. Valitse **Levy**. Tämän jälkeen sinua pyydetään asentamaan ohjainlevy.
9. Napsauta **Selaa** ja valitse oikea Brother-tulostinohjain, joka löytyy CD-ROM-levyltä tai jaetuista resursseista.
   Valitse **OK**.
10. Valitse **OK**.
11. Valitse laitteesi ja valitse **OK**.
12. Valitse **Kyllä**, jos haluat käyttää tätä laitetta oletustulostimena. Napsauta **Seuraava**.
13. Napsauta **Valmis**. Nyt laiteen asetukset on määritetty ja sillä voidaan tulostaa. Voit kokeilla tulostusyhteyttä tulostamalla testisivun.

Windows Vista®, Windows® 7 ja Windows Server® 2008

1. (Windows Vista®)
   Napsauta -painiketta, **Ohjauspaneeli**, **Laitteisto ja äänet** ja sitten **Tulostimet**.
   (Windows® 7)
   Napsauta ja napsauta **Laitteet ja tulostimet**.
   (Windows Server® 2008)
   Valitse **Start** (Käynnistä), **Control Panel** (Ohjauspaneeli), **Laitteisto ja äänet**ja valitse sitten **Printers** (Tulostimet).
2. Valitse **Lisää tulostin**.
3. Valitse **Lisää verkko-, Bluetooth-, tai langaton tulostin** .
4. Valitse **Haluamani tulostin ei ole luettelossa**.
5. Valitse **Valitse jaettu tulostin nimen perusteella** ja syötä seuraava osoite URL-kenttään:
   ”http://laitteen IP-osoite/ipp” (jossa ”laitteen IP-osoite” on laitteen IP-osoite tai solmun nimi.)

Vinkki

- On tärkeää, että käytät muotoa ”https://” muodon ”http://” sijasta. Muutoin IPP:n kautta tulostaminen ei ole suojattua.
- Jos olet muokannut hosts-tiedostoa tietokoneellasi tai käytät Domain Name System (DNS) -järjestelmää, voit myös syöttää tulostuspalvelimen DNS-nimen. Koska tulostuspalvelin tukee TCP/IP:tä sekä NetBIOS-nimiä, voit myös syöttää tulostuspalvelimen NetBIOS-nimen. NetBIOS-nimi näkyy verkkoasetusraportissa. (Jos haluat lisätietoja verkkoasetusraportin tulostamisesta, katso *Tulostusasetukset-sivun tulostaminen (HL-5450DN(T))* ➤➤ sivulla 29 tai *Verkkoasetusraportin tulostaminen (muut mallit)* ➤➤ sivulla 29.) Annettu NetBIOS-nimi on silmukan nimen 15 ensimmäistä merkkiä, ja se näkyy oletusarvoisesti muodossa ”BRNxxxxxxxxxxxx” langallisessa verkossa tai ”BRWxxxxxxxxxxxx” langattomassa verkossa. (”xxxxxxxxxxxx” on laitteesi MAC-osoite/Ethernet-osoite.)

6. Kun napsautat **Seuraava**, Windows Vista® ja Windows Server® 2008 muodostavat yhteyden määrittämääsi osoitteeseen.
   - Jos tulostinohjain on jo asennettu:

     Näet tulostimen valintanäytön kohdassa Add Printer Wizard (Ohjattu tulostimen lisääminen). Valitse **OK**.

     Jos tietokoneeseesi on jo asennettu sopiva ohjainta, Windows Vista® ja Windows Server® 2008 käyttävät ohjainta automaattisesti. Tässä tapauksessa sinulta kysytään, haluatko tehdä ohjaimesta oletustulostimen, jonka jälkeen ohjattu tulostimen lisääminen viimeistellään. Voit nyt tulostaa.

     Siirry vaiheeseen ⓫.

■ Jos tulostinohjainta EI OLE asennettu:

Yksi IPP-tulostusprotokollan eduista on, että se määrittää tulostimen mallin nimen kun kommunikoit sen kanssa. Kun tiedonsiirto on onnistunut, näet tulostimen mallin nimen automaattisesti. Tämä merkitsee sitä, ettei sinun tarvitse ilmoittaa Windows Vista® ja Windows Server® 2008 -järjestelmille käytettävää tulostimen ohjaintyyppiä.

Siirry vaiheeseen ❼.

7 Jos laitteesi ei ole tuettujen tulostinten listalla, napsauta **Levy**. Tämän jälkeen sinua pyydetään asentamaan ohjainlevy.

8 Napsauta **Selaa** ja valitse oikea Brother-tulostinohjain, joka löytyy CD-ROM-levyltä tai jaetuista resursseista. Valitse **Avaa**.

9 Valitse **OK**.

10 Valitse laitteen mallin nimi. Valitse **OK**.

Vinkki

- Kun Käyttäjätilien valvonta tulee näkyviin, napsauta **Jatka**.
- Jos asentamasi tulostin ei sisällä digitaalista varmennetta, näet varoitusviestin. Napsauta **Asenna silti tämä ohjainohjelmisto** jatkaaksesi asennusta. Tämän jälkeen **Tulostimen lisääminen** viimeistellään.

11 Näet **Kirjoita tulostimen nimi**-näytön **Tulostimen lisääminen**-toiminnossa. Valitse **Aseta oletustulostimeksi** -valintaruutu, jos haluat käyttää laitetta oletustulostimena ja napsauta sitten **Seuraava**.

12 Voit kokeilla tulostusyhteyttä napsauttamalla**Tulosta testisivu** ja sitten **Valmis**. Nyt laiteen asetukset on määritetty ja sillä voidaan tulostaa.

5 Sähköpostin lähettäminen tai vastaanottaminen suojatusti (DCP- ja MFC-mallit)

WWW-pohjaisen hallinnan (Web-selaimen) käyttäminen

Voit määrittää suojatun sähköpostiviestien lähettämisen käyttäjän todennuksen avulla tai sähköpostiviestien lähettämisen ja vastaanottamisen (DCP- ja MFC-mallit) SSL/TLS-yhteyden avulla WWW-pohjainen hallinta -näytössä.

1. Käynnistä WWW-selain.
2. Kirjoita selaimeen ”http://laitteen IP-osoite/” (jossa ”laitteen IP-osoite” on laitteen IP-osoite).
   - Esimerkki:

     http://192.168.1.2/
3. Salasanaa ei oletusarvon mukaan tarvita. Jos olet määrittänyt salasanan, anna se ja paina .
4. Valitse **Network** (Verkko).
5. Valitse **Protocol** (Protokolla).
6. Valitse kohdassa **POP3/SMTP Advanced Setting** (Lisäasetukset) ja varmista, että **POP3/SMTP**-tila on **Enabled** (Ota käyttöön).
7. **POP3/SMTP**-asetukset voidaan määrittää tällä sivulla.

Vinkki

- Katso lisätietoja WWW-pohjaisen hallinnan Ohjeesta.
- Sähköpostiasetukset voidaan myös tarkistaa määrityksen jälkeen lähettämällä testiviesti.
- Jos et tiedä POP3/SMTP-palvelinasetuksia, pyydä tiedot järjestelmänvalvojalta tai Internet-palveluntarjoajalta.

8. Kun asetukset ovat valmiit, valitse **Submit** (Lähetä). **Test E-mail Send Configuration** (Testaa sähköpostin lähetysasetuksia) tai**Test E-mail Send/Receive Configuration** (Testaa sähköpostin lähetys/vastaanottoasetuksia) -näyttö avautuu.
9. Noudata näytöllä annettuja ohjeita, jos haluat testata nykyiset asetukset.

Sähköpostin lähettäminen tai vastaanottaminen suojatusti (DCP- ja MFC-mallit) SSL/TLS-yhteyden avulla

Tämä laite tukee SSL/TLS-menetelmiä sähköpostiviestien lähettämiseksi tai vastaanottamiseksi (DCP- ja MFC-mallit) SSL/TLS-tekniikkaa käyttävän sähköpostipalvelimen kautta. Voit lähettää tai vastaanottaa sähköpostiviestejä SSL/TLS-tekniikkaa käyttävän sähköpostipalvelimen kautta määrittämällä SMTP yli SSL/TLS- tai POP3 yli SSL/TLS -asetukset oikein.

Palvelinvarmenteen todentaminen

- Jos valitset SSL- tai TLS-menetelmän kohdassa **SMTP over SSL/TLS** tai **POP3 over SSL/TLS**, **Verify Server Certificate** (Varmista palvelinvarmenne) -valintaruutu valitaan automaattisesti palvelinvarmenteen todentamiseksi.
  - Ennen palvelinvarmenteen todentamista sinun on tuotava CA-varmenne, jonka on myöntänyt palvelinvarmenteen allekirjoittanut CA. Kysy verkonvalvojalta tai Internet-palveluntarjoajalta, onko CA-varmenteen tuominen tarpeen. Jos haluat lisätietoja varmenteen tuomisesta, katso *CA-varmenteen tuominen ja vieminen* ➤➤ sivulla 18.
  - Jos sinun ei tarvitse todentaa palvelinvarmennetta, poista **Verify Server Certificate** (Varmista palvelinvarmenne) -valintaruudun valinta.

Portin numero

- Jos valitset SSL- tai TLS-yhteyden, **SMTP Port** (SMTP-portti)- tai **POP3 Port** (POP3-portti)-arvo muutetaan vastaamaan protokollaa. Jos haluat muuttaa portin numeroa manuaalisesti, anna portin numero, kun olet valinnut **SMTP over SSL/TLS** tai **POP3 over SSL/TLS**.
- Sinun on määritettävä POP3/SMTP-tietoliikennemenetelmä vastaamaan sähköpostipalvelinta. Pyydä lisätietoja sähköpostipalvelimen asetuksista verkonvalvojalta tai Internet-palveluntarjoajalta. Useimmissa tapauksissa suojatut webmail-palvelut vaativat seuraavat asetukset:
  - **SMTP**
    - **SMTP-portti**: 587
    - **SMTP Server Authentication Method** (SMTP-palvelimen varmennustapa): SMTP-AUTH
    - **SMTP over SSL/TLS**: TLS
  - **POP3**
    - **POP3-portti**: 995
    - **POP3 over SSL/TLS**: SSL

6 Vianetsintä

Yleistä

Tässä luvussa kerrotaan, miten Brother-laitetta käytettäessä mahdollisesti esiin tulevat tyypilliset verkko-ongelmat ratkaistaan. Jos et tämän luvun luettuasi pysty ratkaisemaan ongelmaasi, vieraile Brother Solutions Centerissä osoitteessa: (http://solutions.brother.com/).

Voit ladata muut ohjeet siirtymällä Brother Solutions Centeriin osoitteessa (http://solutions.brother.com/) ja napsauttamalla oman mallisi sivulla Käyttöohjeet.

Ongelman tunnistaminen

Varmista ennen tämän luvun lukemista, että seuraavat on määritetty oikein.

Varmista ensin seuraavat:
Virtajohto on kytketty oikein ja Brother-laitteen virta on kytketty.
Kaikki suojamateriaali on poistettu laitteesta.
Värikasetit ja rumpuyksikkö on asennettu oikein.
Etu- ja takakannet ovat täysin kiinni.
Paperi on asetettu oikein paperikasettiin.
Laite yhdistetty verkkoon oikein.

Siirry ratkaisusi sivulle alla olevassa luettelossa

- En voi tulostaa asiakirjaa Internetin välityksellä IPPS-protokollan avulla.

  Katso *En voi tulostaa asiakirjaa Internetin välityksellä IPPS-protokollan avulla.* ➤➤ sivulla 28.

- Haluan tarkistaa, että verkkolaitteet toimivat oikein.

  Katso *Haluan tarkistaa, että verkkolaitteet toimivat oikein.* ➤➤ sivulla 28.

En voi tulostaa asiakirjaa Internetin välityksellä IPPS-protokollan avulla.

Kysymys	Ratkaisu
En voi kommunikoida Brother-laitteen kanssa SSL-protokollan avulla.	■ Hanki oikea varmenne ja asenna se sekä laitteeseesi että tietokoneeseesi uudelleen. ■ Varmista, että laitteesi porttiasetus on määritetty oikein. Voit varmistaa laitteesi porttiasetukset WWW-pohjaisen hallinnan näytössä valitsemalla ensin **Network** (Verkko), **Protocol** (Protokolla) ja sitten **HTTP Server Settings** (HTTP-palvelimen asetukset).

Haluan tarkistaa, että verkkolaitteet toimivat oikein.

Kysymys	Ratkaisu
Onko Brother-laitteesi kytketty päälle?	Tarkista, että olet varmistanut kaikki kohdan *Varmista ensin seuraavat:* ➤➤ sivulla 27 ohjeet.
Mistä löydän Brother-laitteen verkkoasetukset, esimerkiksi IP-osoitteen?	Tulosta verkkoasetusraportti. Katso *Tulostusasetukset-sivun tulostaminen (HL-5450DN(T))* ➤➤ sivulla 29 tai *Verkkoasetusraportin tulostaminen (muut mallit)* ➤➤ sivulla 29.

Tulostusasetukset-sivun tulostaminen (HL-5450DN(T))

Vinkki

Solmun nimi: Solmun nimi näkyy verkkoasetusluettelossa. Solmun oletusnimi on ”BRNxxxxxxxxxxxx”. (”xxxxxxxxxxxx” on laitteesi MAC-osoite/Ethernet-osoite.)

Tulostusasetukset-sivu tulostaa raportin, jossa luetellaan kaikki nykyiset käytössä olevat tulostusasetukset, mukaan lukien verkkotulostuspalvelimen asetukset.

Voit tulostaa Tulostusasetukset-sivun laitteen **Go**-painikkeen avulla.

1. Varmista, että etukansi on suljettu ja virtajohto on kytketty.
2. Kytke laitteeseen virta ja odota, kunnes laite on toimintavalmis.
3. Paina **Go**-näppäintä kolme kertaa 2 sekunnin sisällä. Laite tulostaa nykyisen Tulostusasetukset-sivun.

Verkkoasetusraportin tulostaminen (muut mallit)

Vinkki

Solmun nimi: Solmun nimi näkyy verkkoasetusluettelossa. Solmun oletusnimi on ”BRNxxxxxxxxxxxx” langallisessa verkossa ja ”BRWxxxxxxxxxxxx” langattomassa verkossa. (”xxxxxxxxxxxx” on laitteesi MAC-osoite/Ethernet-osoite.)

Verkkoasetusraporttiin tulostuvat kaikki verkon voimassa olevat asetukset, myös verkon tulostuspalvelimen asetukset.

HL-5470DW(T)- ja HL-6180DW(T)-laitteelle

1. Valitse `Laitetiedot` painamalla ▲ tai ▼.
   Paina **OK**.
2. Valitse `Tul. NetSetting` painamalla ▲ tai ▼.
   Paina **OK**.

DCP-8110DN, DCP-8150DN, DCP-8155DN, MFC-8510DN, MFC-8710DW ja MFC-8910DW

1. Paina **Menu**.
2. (MFC-mallit) Valitse `Tulosta rap.` painamalla ▲ tai ▼.
   (DCP-mallit) Valitse `Laitetiedot` painamalla ▲ tai ▼.
   Paina **OK**.
3. Valitse `Verkkoasetuk.` painamalla ▲ tai ▼.
   Paina **OK**.
4. Paina **Start**.

DCP-8250DN- ja MFC-8950DW(T)-laitteelle

1. Paina `Valik.`
2. Tuo `Tulosta rap.` näyttöön painamalla ▲ tai ▼ ja paina sitten `Tulosta rap.`.
3. Paina `Verkkoasetuk.`.
4. Paina **Start**.

Vinkki

Jos verkkoasetusraportissa **IP Address** on arvoltaan **0.0.0.0**, odota yksi minuutti ja yritä uudelleen.

Verkkosanasto ja -käsitteet

SSL-protokollan tekninen kuvaus

SSL (Secure Socket Layer) on kuljetuskerroksessa olevien tietojen suojausmenetelmä, joka suojaa tiedonsiirtoa paikallisessa tai laajassa verkossa IPP (Internet Printing Protocol) -protokollan avulla estäen luvattomia käyttäjiä lukemasta tietoja.

Protokolla tarjoaa suojauksen digitaalisia avaimia hyödyntävillä todennusprotokollilla. Digitaalisia avaimia on 2:

- Julkinen avain – avaimen tuntee kaikki tulostimen käyttäjät.
- Yksityinen avain – avaimen tuntee ainoastaan pakettien salaukseen käytetty laite, joka pystyy myös muuttamaan paketit luettavaan muotoon.

Julkinen avain käyttää joko 1024-bittistä tai 2048-bittistä salausta sisältyen yhteen digitaaliseen varmenteeseen. Nämä varmenteet voivat olla joko itse allekirjoitettuja tai CA-varmenteita.

Avaimia on olemassa kolmea erityyppiä: yksityinen, julkinen ja jaettu.

Yksityinen avain, jonka tuntee ainoastaan laite, liittyy julkiseen avaimeen, mutta se ei sisälly työaseman (lähettäjän) digitaaliseen varmenteeseen. Kun käyttäjä luo yhteyden ensimmäistä kertaa, laite lähettää julkisen avaimen yhdessä varmenteen kanssa. Työasema luottaa, että julkinen avain on lähtöisin varmenteen omaavasta laitteesta. Työasema luo jaetun avaimen koodaten sen julkiseen avaimeen ja lähettää sen laitteeseen. Laite koodaa jaetun avaimen yksityiseen avaimeen. Nyt laite ja työasema jakavat jaetun avaimen turvallisesti ja luovat turvallisen yhteyden tulostustietojen siirtoon.

Tulostustiedot koodataan ja avataan jaetulla avaimella.

SSL ei estä luvattomien käyttäjien pääsyä paketteihin, mutta protokolla tekee paketeista lukukelvottomia ilman yksityistä avainta, joka välitetään ainoastaan laitteelle.

Salaus voidaan määrittää sekä langallisiin että langattomiin verkkoihin ja se toimii myös muiden suojausmenetelmien, kuten WPA-avainten ja palomuurien kanssa asianmukaisilla määrityksillä.

Verkkosanasto

- SSL (Secure Socket Layer)

  Tietoliikenteen suojausprotokolla, joka ehkäisee tietoturvauhkia salaamalla tietoja.

- IPP (Internet Printing Protocol)

  IPP on yleinen tulostusprotokolla, jota käytetään tulostustöiden hallintaan. Sitä voidaan käyttää sekä paikallisesti että maailmanlaajuisesti, eli kuka tahansa ympäri maailmaa voi tulostaa saman laitteen kautta.

- IPPS

  IPP (Internet Printing Protocol, versio 1.0) -tulostusprotokollan versio, joka käyttää SSL:ää.

- HTTPS

  HTTP (Hyper Text Transfer Protocol) -Internet-protokollan versio, joka käyttää SSL:ää.

- CA (Certificate Authority)

  CA on taho, joka myöntää digitaalisia varmenteita (erityisesti X.509-varmenteita) ja takaa varmenteiden tieto-osien väliset sidokset.

- CSR (Certificate Signing Request)

  CSR on CA:lle lähetetty viesti, jossa hakija anoo varmenteen myöntämistä. CSR sisältää hakijan tunnistetiedot, hakijan luoman julkisen avaimen sekä hakijan digitaalisen allekirjoituksen.

- Varmenne

  Varmenne on julkisen avaimen ja identiteetin yhdistävät tiedot. Varmenteella voidaan varmistaa, että julkinen avain kuuluu jollekin tietylle henkilölle. Muoto määräytyy x.509-standardin mukaan.

- Julkisen avaimen salausjärjestelmä

  Julkisen avaimen salausjärjestelmä on salausmenetelmien uusi haara, jossa algoritmit hyödyntävät avainpareja (julkista ja yksityistä avainta) ja käyttävät parin eri osia algoritmin eri vaiheissa.

- Jaetun avaimen salausjärjestelmä

  Jaetun avaimen salausjärjestelmä on salausmenetelmien uusi haara, jossa käytetään algoritmeja siten, että ne käyttävät samaa avainta algoritmin eri vaiheissa (kuten salauksessa ja salauksen purkamisessa).